DETAILED ACTION

Examiner's Amendment

1. An Examiner's amendment to the record appears below. Should the changes and/or additions by unacceptable to applicant, an amendment may be filed as provided by 37 C.F.R. §1.312. To ensure consideration of such amendment, it must be submitted no later than the payment of the issue fee.

2. Authorization for this Examiner's amendment was given in a telephonic communication with Robert Maier (Registration No. 54,291) on or about May 21, 2010.

3. The application has been amended as follows:

Listing of Claims

1. (Currently Amended) A system for authenticating a cardholder transaction with a merchant on an electronic network, the system comprising:

an issuer platform layer including at least one 3-D Secure authentication program;

a merchant plug-in (MPI);

an secure payment algorithm (SPA); and

and a data transport layer, wherein the issuer platform comprises an access control server (ACS) that uses the SPA to process transaction and cardholder information for authentication by an authentication method and to generate an Accountholder Authentication Value (AAV) and

conveys the AAV through the data transport layer to the MPI, wherein the AAV is a formatted data structure compatible with 3-D Secure message protocols, wherein the formatted data structure has a length of at most 20-bytes including bytes that identify a hash of the merchant's name, bytes that identify the ACS, bytes that identify the authentication method, bytes that identify secret cryptographic keys and bytes that include a merchant authentication code (MAC),

wherein the SPA comprises an encryption algorithm for generating the MAC, wherein the encryption algorithm uses a pair of secret keys A and B that are identified in the AAV to encrypt a concatenation of the card holder's account number, card expiration date and service code to generate a three-digit CVC2 field, and uses the result to populate two bytes of the MAC.

2. (Previously Presented) The system of claim 1 wherein the AAV is a formatted data structure that is Base 64 encoded.

3. (Previously Presented) The system of claim 1, wherein the SPA comprises an encryption algorithm for generating the MAC, wherein the encryption algorithm uses a secret key identified in the AAV to encrypt a concatenation of the card holder's account number and a plurality of the fields of the bytes of the AAV excluding bytes that represent the MAC, and wherein a portion of the encryption result forms the MAC bytes in the AAV.

4. (Canceled)

5. (Previously Presented) The system of claim 1 wherein the pair of secret keys A and B are 64-bit Data Encryption Standard (DES) keys.

6. (Previously Presented) The system of claim 1 wherein the ACS is configured to generate an AAV in response to a payment authentication request message from the MPI to the ACS.

7. (Previously Presented) The system of claim 1, which is configured to transport the AAV in a payment authentication response message from the ACS.

8. (Previously Presented) The system of claim 7 wherein the ACS is further configured to place a digital signature on the payment authentication response message.

9. (Previously Presented) The system of claim 1 wherein the MPI is configured to verify the digital signature on a received payment authentication response message.

10. (Previously Presented) The system of claim 1 wherein the MPI is configured to extract the MAC fields included in a payment authentication response message from the ACS and to place the extracted MAC in a payment authorization request message to a third party.

11. (Currently Amended) A data structure for conveying cardholder transaction authentication information amongst stakeholders in a 3-D Secure environment, the data structure comprising 20 bytes of Base 64 encoded characters, wherein the first byte is a control byte, bytes 2-9 represent a hash of a merchant name, byte 10 identifies an Access control server (ACS) that authenticates the cardholder transaction by an authentication method, byte 11 identifies the authentication method and the secret encryption keys that are used by the ACS to generate a Merchant Authentication Code (MAC), bytes 12-15 represent a transaction sequence number identifying a transaction number processed by the ACS, and bytes 16-20 represent the MAC_2

wherein the MAC comprises portions of an encryption of a concatenation of the card holder's account number, card expiration date and service code, and wherein a pair of keys A and B that are identified in byte 11 is used for encryption..

12. (Previously Presented) The data structure of claim 11 wherein the MAC comprises portions of an encryption of a concatenation of the card holder's account number and a plurality of the fields of bytes 1-15 of the data structure, and wherein a single key identified in byte 11 is used for encryption.

13. (Canceled)

14. (Previously Presented) The data structure of claim 11 wherein a three-digit encryption result is used to populate two bytes of the MAC bytes 16-20.

15. (Previously Presented) The data structure of claim 11 wherein the pair of secret keys A and B are 64 bit Data Encryption Standard (DES) keys.

16. (Currently Amended) A method for authenticating a cardholder transaction with a merchant on an electronic network in an 3-D Secure environment, the method comprising:

using an Access control server (ACS) to process cardholder and transaction information to authenticate the cardholder by an authentication method;

deploying a secure payment algorithm (SPA) to generate an Accountholder Authentication Value (AAV) to represent the authentication results, and transporting the AAV in 3-D Secure messages to the merchant, wherein the AAV is a formatted data structure that has a length of at most 20 bytes, including bytes that identify a hash of the merchant's name, bytes that

identify the ACS, bytes that identify the authentication method, bytes that include a merchant authentication code (MAC), and bytes that identify secret cryptographic keys that are used by the SPA to generate MAC_a

wherein deploying a SPA comprises:

using a pair of pair secret keys A and B that are identified in the AAV to encrypt a concatenation of the card holder's account number, card expiration date and service code to generate a three-digit CVC2 field; and

assigning the result to populate two bytes of the MAC.

17. (Previously Presented) The method of claim 16 wherein the AAV is a formatted data structure that is Base 64 encoded.

18. (Previously Presented) The method of claim 16 wherein deploying a SPA comprises:

using a secret key identified in the AAV to encrypt a concatenation of the card holder's account number and at least portions of the bytes of the AAV excluding bytes that represent the MAC; and

assigning a portion of the encryption result to the MAC bytes in the AAV.

19. (Canceled)

20. (Previously Presented) The method of claim 17 wherein the pair of secret keys A and B are 64 bit Data Encryption Standard (DES) keys.

21. (Previously Presented) The method of claim 16 wherein transporting the AAV in 3-D Secure messages to the merchant comprises transporting the AAV in a payment authentication response message that is digitally signed by the ACS.

22. (Previously Presented) The method of claim 21, further comprising:

first, verification by the merchant of the digital signature on a received payment authentication response message; and

next, extraction of the MAC fields from the received payment authentication response message by the merchant.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shahid Kamal whose telephone number is (571) 270-3272. The Examiner can normally be reached on Mon-Thursday 8:30 AM- 7:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Peter Vo can be reached on (571) 272-4690. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Shahid Kamal/
Examiner, Art Unit 3714

/Pierre E. Elisca/
Primary Examiner, Art Unit 3714